

NIL IDEALS IN GROUP RINGS

D. S. Passman

Let R be a commutative ring having no nonzero nilpotent elements. We consider nil ideals in the group ring $R[G]$. In this paper conditions on G and R are found that ensure that $\text{Nil } R[G]$, the upper nil radical of the group ring, is trivial. We also obtain necessary and sufficient conditions for the existence of nontrivial nilpotent ideals. In the particular case where R is a field K , the above results yield sufficient conditions on G and K for the semi-simplicity of the group algebra $K[G]$. These are similar to and, in fact, motivated by the results of S. A. Amitsur in [1] for fields of characteristic zero.

If there exists a positive integer \bar{m} with $\bar{m}R = (0)$, then we set $\text{ch } R$, the characteristic of R , equal to the smallest such positive integer. Otherwise, $\text{ch } R = 0$. In the first case, let $\pi(R) = \{p_1, p_2, \dots, p_k\}$ be the set of prime divisors of $m = \text{ch } R$. Then since R has no nontrivial nilpotent elements, it is immediate that each prime occurs only to the first power. The integers $m/p_1, m/p_2, \dots, m/p_k$ are relatively prime, so there is a linear sum

$$n_1 m/p_1 + n_2 m/p_2 + \dots + n_k m/p_k = 1.$$

This induces a decomposition

$$R = R_{p_1} \dot{+} R_{p_2} \dot{+} \dots \dot{+} R_{p_k}$$

of R as an internal direct sum of nonzero ideals, where

$$R_{p_i} = n_i m/p_i R = \{r \in R: p_i r = 0\}.$$

Hence, for any group G ,

$$R[G] = R_{p_1}[G] \dot{+} R_{p_2}[G] \dot{+} \dots \dot{+} R_{p_k}[G].$$

An ideal of the group ring is then nil or nilpotent if and only if its projection into each factor is. This effectively reduces all $\text{ch } R \neq 0$ considerations to the prime case.

We say an element $\sigma \in G$ is a p element if it is of order p^j for some $j \geq 1$.

THEOREM I. *Let R be a commutative ring having no nonzero nilpotent elements. Suppose that $\text{ch } R \neq 0$ and that G has no p elements for all $p \in \pi(R)$. Then $\text{Nil } R[G] = (0)$.*

First, we need a few lemmas. Let Γ be any ring. We write $\text{Comm } \Gamma$ for the commutator of Γ , the set of all finite sums of elements of the form $ab - ba$ with $a, b \in \Gamma$.

LEMMA 1. *Let p be a prime, and let k and n be arbitrary positive integers. Then for all $x_1, x_2, \dots, x_n \in \Gamma$,*

$$(x_1 + x_2 + \cdots + x_n)^{p^k} = x_1^{p^k} + x_2^{p^k} + \cdots + x_n^{p^k} + p\gamma + z,$$

where $\gamma \in \Gamma$ and $z \in \text{Comm } \Gamma$.

Proof. Observe that

$$(x_1 + x_2 + \cdots + x_n)^{p^k} = x_1^{p^k} + x_2^{p^k} + \cdots + x_n^{p^k} + t,$$

where t is the sum of all words of the form

$$x_{i_1} x_{i_2} \cdots x_{i_{p^k}}$$

with at least two different subscripts occurring.

If words w_1 and w_2 are cyclic permutations of each other, that is, if

$$w_1 = x_{i_1} x_{i_2} \cdots x_{i_{p^k}},$$

$$w_2 = x_{i_j} x_{i_{j+1}} \cdots x_{i_{p^k}} x_{i_1} \cdots x_{i_{j-1}},$$

then

$$w_1 - w_2 = ab - ba \in \text{Comm } \Gamma, \quad \text{with}$$

$$a = x_{i_1} x_{i_2} \cdots x_{i_{j-1}}, \quad b = x_{i_j} x_{i_{j+1}} \cdots x_{i_{p^k}}.$$

Hence, modulo $\text{Comm } \Gamma$ all cyclic permutations of a word w are congruent. But an easy counting argument shows that the number of such words is divisible by p . Thus the result follows.

For convenience we introduce the following notation. For all

$$a = \sum r_\sigma \sigma \in R[G],$$

we set $\theta(a) = r_1$, the coefficient of the identity of G .

Now $\text{Comm } R[G]$ is spanned over R^2 by all elements of the form $\sigma\tau - \tau\sigma$ with $\sigma, \tau \in G$. But $\sigma\tau = 1$ if and only if $\tau\sigma = 1$, so we have proved

LEMMA 2. *If $z \in \text{Comm } R[G]$, then $\theta(z) = 0$.*

LEMMA 3. *Let R be a commutative ring having no nonzero nilpotent elements, and let $\text{ch } R = p > 0$. If*

$$a = r_1 1 + r_2 \sigma_2 + \cdots + r_n \sigma_n \in R[G]$$

is nilpotent and no σ_i is a p element, then $\theta(a) = r_1 = 0$.

Proof. Suppose $a^{p^k} = 0$. Then

$$0 = a^{p^k} = r_1^{p^k} 1 + r_2^{p^k} \sigma_2^{p^k} + \cdots + r_n^{p^k} \sigma_n^{p^k} + pb + z$$

by Lemma 1. Now $pb = 0$ since $\text{ch } R = p$ and, by assumption, no $\sigma_i^{p^k}$ is equal to 1. Hence,

$$r_1^{p^k} = -\theta(z) = 0$$

by Lemma 2. Therefore $r_1 = 0$.

Proof of theorem. It suffices to show that for each $p \in \pi(R)$, $\text{Nil } R_p[G] = (0)$. But R_p has characteristic p , and G has no p elements. If

$$a = \sum r_\sigma \sigma \in \text{Nil } R_p[G],$$

then for all $\tau \in G$, $a\tau^{-1}$ is nilpotent. Therefore by the preceding lemma, $\theta(a\tau^{-1}) = r_\tau = 0$. Hence, $a = 0$.

For the case where $\text{ch } R$ is zero, we have the following result.

THEOREM II. *Let R be a commutative ring without nonzero nilpotent elements. Suppose $(R, +)$ is torsion free. Then for any group G , $\text{Nil } R[G] = (0)$.*

We first consider a special case.

LEMMA 4. *Let K be a finite field extension of the rational numbers \mathbb{Q} . Then $\text{Nil } K[G] = (0)$.*

Proof. Let D be the integral closure in K of the rational integers \mathbb{Z} . Then K is the quotient field of D .

Suppose $\text{Nil } K[G] \neq (0)$. Then by multiplying by a suitable group element and a field element, we can suppose

$$\alpha = d_1 1 + d_2 \sigma_2 + \cdots + d_n \sigma_n \in D[G]$$

is nilpotent and $d_1 \neq 0$.

The norm map $N_{K/\mathbb{Q}}$ maps D into \mathbb{Z} , and by assumption, $N_{K/\mathbb{Q}}(d_1) \neq 0$. Choose a prime p with

- $p > \text{absolute value of } N_{K/\mathbb{Q}}(d_1),$
- $> \text{all the finite orders of the } \sigma_i,$
- $> \text{the degree of nilpotence of } \alpha .$

Then

$$0 = \alpha^p = d_1^p 1 + d_2^p \sigma_2^p + \cdots + d_n^p \sigma_n^p + p\beta + z,$$

where $\beta \in D[G]$ and $z \in \text{Comm } D[G]$. Hence $d_1^p = pd$ with $d = -\theta(\beta)$ by Lemma 2.

Thus if $t = [K:\mathbb{Q}]$,

$$N_{K/\mathbb{Q}}(d_1)^p = N_{K/\mathbb{Q}}(d_1^p) = N_{K/\mathbb{Q}}(pd) = p^t N_{K/\mathbb{Q}}(d).$$

But p does not divide $N_{K/\mathbb{Q}}(d_1)$, so this is the required contradiction.

To reduce the general problem to this special case, we need the following two lemmas, whose proofs are immediately clear.

LEMMA 5. Let $R^\#$ be the canonical ring extension of R having a unit element. Then $\text{Nil } R[G] \subseteq \text{Nil } R^\#[G]$.

LEMMA 6. Let S be a multiplicative subset of regular elements (nonzero divisors) of R . Then $\text{Nil } S^{-1}R[G] = S^{-1}\text{Nil } R[G]$.

Proof of theorem. By Lemma 5, we can suppose that R contains a unit element. The hypotheses of the theorem state precisely that the nonzero integers Z_* in R form a multiplicative subset of regular elements. So by the preceding lemma, we need only consider the ring $Z_*^{-1}R$, or in other words, we can assume that R is a unitary over-ring of the rationals Q . Note that neither of these extensions of R can introduce nonzero nilpotent elements in the ring.

The result now follows by the Hilbert Nullstellensatz. Let

$$\alpha = r_1 \sigma_1 + r_2 \sigma_2 + \cdots + r_n \sigma_n \in \text{Nil } R[G],$$

and let $\bar{R} = Q[r_1, r_2, \dots, r_n] \subseteq R$. Then $\alpha \in \text{Nil } \bar{R}[G]$. Let M be a maximal ideal of \bar{R} . The image of α under the map

$$\bar{R}[G] \rightarrow \bar{R}/M[G]$$

is an element of $\text{Nil } \bar{R}/M[G]$. But \bar{R}/M is a finite algebraic extension of Q , so by Lemma 4, the image is zero.

Hence, $r_1, r_2, \dots, r_n \in M$ for all maximal ideals M . That is the r_i belong to the Jacobson radical of \bar{R} . But \bar{R} is a finitely generated commutative algebra, and a second application of the Nullstellensatz implies that r_1, r_2, \dots, r_n are nilpotent. Finally, since R has no nonzero nilpotent elements, $\alpha = 0$.

Now, Theorem I yields sufficient conditions for the nil radical to be zero. That it need not be zero can be seen from the following example.

Let A be an abelian group having no elements of even order, and let $X = \{1, x\}$ be a group of order two. Set G equal to the semi-direct product of A by X , where x acts on A by sending each element to its inverse. We consider $K[G]$ for K a field of characteristic two.

PROPOSITION. *With the above notation,*

(i) if A is finite, $\text{Nil } K[G] = K \cdot (\sum_{\rho \in G} \rho)$;

(ii) if A is infinite, $\text{Nil } K[G] = (0)$.

Proof. We use the notation $a, b \in K[A]$ so that any element of $K[G]$ can be written uniquely as $a + bx$. If $a = \sum_{\sigma \in A} k_\sigma \sigma$, we set $a^{-1} = \sum_{\sigma \in A} k_\sigma \sigma^{-1}$. Notice that $ax = xa^{-1}$.

Now, if a is nilpotent, then since $K[A]$ is commutative, a generates a nil ideal in $K[A]$. But by Theorem I, $\text{Nil } K[A] = (0)$, so in this case $a = 0$.

Let $a + bx \in \text{Nil } K[G]$, then

$$\begin{aligned} (a + bx)(a^{-1} + bx) &= (aa^{-1} + bxbx) + (bxa^{-1} + abx), \\ &= (aa^{-1} + bb^{-1}) + (ba + ab)x, \\ &= (aa^{-1} + bb^{-1}) \in \text{Nil } K[G]. \end{aligned}$$

Thus $aa^{-1} = bb^{-1}$ since $\text{ch } K = 2$.

Therefore,

$$\begin{aligned} (a + bx)^2 &= (aa + bxbx) + (abx + bxa), \\ &= (aa + bb^{-1}) + (abx + a^{-1}bx), \\ &= (aa + aa^{-1}) + (abx + a^{-1}bx), \\ &= (a + a^{-1})(a + bx). \end{aligned}$$

Thus if $(a + bx)^m = 0$,

$$0 = (a + a^{-1})^{m-1}(a + bx)$$

so that $(a + a^{-1})^{m-1}a = 0$. Moreover,

$$(a + a^{-1})^{m-1}a^{-1} = x[(a + a^{-1})^{m-1}a]x = 0.$$

Therefore, by addition, $(a + a^{-1})^m = 0$. Hence $a + a^{-1}$ is nilpotent, so $a = a^{-1}$.

Now if $\sigma \in A$, then

$$\sigma(a + bx) \in \text{Nil } K[G],$$

and $\sigma a = (\sigma a)^{-1}$. Suppose $a \neq 0$, and choose σ so that $\theta(\sigma a) \neq 0$. Then since 1 is the only element of A which is its own inverse, the number of nonzero terms of σa , and hence of a , is odd since $(\sigma a) = (\sigma a)^{-1}$. But if $\tau \in A$ and the coefficient of τ in a is zero, then $\theta(\tau^{-1}a) = 0$, which implies that the number of nonzero terms is even. Therefore, all elements of A must appear.

Thus if A is infinite, $a = 0$ and $(bx)x = b \in \text{Nil } K[G]$. Consequently, $b = 0$. Therefore (ii) is proved.

Now assume A is finite and thus is of odd order. Then every element of A has a square root. Suppose $a = \sum_{\sigma \in A} k_{\sigma} \sigma$. Fix $\sigma_1, \sigma_2 \in A$, and choose τ so that $\tau^2 = \sigma_1^{-1} \sigma_2^{-1}$. Then $\tau \sigma_1 = (\tau \sigma_2)^{-1}$. But $(\tau a) = (\tau a)^{-1}$, so $k_{\sigma_1} = k_{\sigma_2}$. Hence $a = k \sum_{\sigma \in A} \sigma$.

We also see that

$$(a + bx)x = b + ax \quad \text{in } \text{Nil } K[G],$$

so we obtain similarly the result that $b = \bar{k} \sum_{\sigma \in A} \sigma$. Clearly,

$$z = \bar{k} \sum_{\rho \in G} \rho \in \text{Nil } K[G];$$

therefore,

$$(a + bx) - z = (k - \bar{k}) \sum_{\sigma \in A} \sigma$$

is nilpotent. Hence $k = \bar{k}$, and (i) is proved.

Necessary and sufficient conditions for the existence of nontrivial nil ideals in $R[G]$ are not immediately apparent. However we have found them for nilpotent ideals.

THEOREM III. *Let R be a commutative ring having no nonzero nilpotent elements and such that $\text{ch } R \neq 0$. Then $R[G]$ has a nontrivial nilpotent ideal if and only if G contains a finite normal subgroup H whose order is divisible by some $p \in \pi(R)$.*

LEMMA 7. *Let J be a group, and let H_1, H_2, \dots, H_n be a finite number of its subgroups. Suppose there exists a finite collection of elements $\sigma_{ij} \in J$ ($i = 1, 2, \dots, n; j = 1, 2, \dots, f(i)$) with*

$$J = \bigcup_{i,j} H_j \sigma_{ij} \quad (\text{The union is set theoretic.})$$

Then for some index i , $[J: H_i] < \infty$.

Proof. By relabeling, we can assume all the H_i to be distinct. We prove the result by induction on n , the number of distinct H_i . The case $n = 1$ is clear.

If a full set of cosets of H_n appears among the $H_n \sigma_{nj}$, then $[J: H_n] < \infty$, and we are finished. Otherwise, if $H_n \tau$ is a missing coset, then

$$H_n \tau \subseteq \bigcup_{i,j} H_i \sigma_{ij}.$$

But $H_n \tau \cap H_n \sigma_{nj}$ is empty, so

$$H_n \tau \subseteq \bigcup_{\substack{i \neq n \\ j}} H_i \sigma_{ij}.$$

Thus all the cosets $H_n \sigma_{nj}$ can be replaced by finite unions of cosets of the remaining H_i . Doing this yields a representation of J in terms of a smaller number of subgroups, and the result follows.

For any group G set

$$\Delta = \{ \sigma \in G: \sigma \text{ has only a finite number of conjugates in } G \}.$$

If σ_1, σ_2 lie in Δ , then so does $\sigma_1 \sigma_2^{-1}$, since for any $\tau \in G$

$$\tau^{-1} (\sigma_1 \sigma_2^{-1}) \tau = [\tau^{-1} \sigma_1 \tau] [\tau^{-1} \sigma_2 \tau]^{-1},$$

and there are only a finite number of possibilities for each factor. Thus Δ is a subgroup of G , and it is clearly characteristic.

We denote by ψ the projection of $R[G]$ into $R[\Delta]$, that is,

$$\psi: R[G] \rightarrow R[\Delta].$$

If $\alpha = \sum r_\sigma \sigma \in R[G]$, then

$$\psi(\alpha) = \sum_{\sigma \in \Delta} r_\sigma \sigma \in R[\Delta].$$

For convenience, given $\alpha = \sum r_\sigma \sigma \in R[G]$, we write

$$\text{Supp } \alpha = \{ \sigma \in G: r_\sigma \neq 0 \},$$

which is the support of α .

LEMMA 8. *Let $\alpha \in R[G]$, and suppose that for all $\sigma \in G$*

$$\psi(\sigma^{-1} \alpha \sigma) = 0.$$

Then if $\alpha_0 = \psi(\alpha)$, $\alpha_0^2 = 0$.

Proof. Write $\alpha = \alpha_0 + \beta$, where

$$\beta = r_1 \tau_1 + \dots + r_n \tau_n \quad (\tau_i \notin \Delta).$$

For each $\rho \in \text{Supp } \alpha_0$, $[G: C(\rho)] < \infty$, $C(\rho)$ being the centralizer of ρ . Let

$$J = \bigcap_{\rho \in \text{Supp } \alpha_0} C(\rho).$$

Then $[G: J] < \infty$; and for all $\sigma \in J$, $\sigma^{-1} \alpha_0 \sigma = \alpha_0$. Set $H_i = J \cap C(\tau_i)$ ($i = 1, 2, \dots, n$).

Assume $\alpha_0^2 \neq 0$, and choose a $\xi \in \text{Supp } \alpha_0^2$. For each i , if τ_i is conjugate to $\xi \tau_j^{-1}$ by an element of J , choose $\sigma_{ij} \in J$ so that

$$\sigma_{ij}^{-1} \tau_i \sigma_{ij} = \xi \tau_j^{-1}.$$

Let $\sigma \in J$. Then

$$\begin{aligned} \sigma^{-1} \alpha \sigma &= (\alpha_0 + \sigma^{-1} \beta \sigma) (\alpha_0 + \beta), \\ &= \alpha_0^2 + \sigma^{-1} \beta \sigma \alpha_0 + \alpha_0 \beta + \sigma^{-1} \beta \sigma \beta. \end{aligned}$$

Now $\psi(\sigma^{-1} \alpha \sigma) = 0$. Hence the ξ term of α_0^2 must be cancelled out by a ξ term in one of the remaining three summands. Thus it is clear, since

$$\text{Supp } (\sigma^{-1} \beta \sigma \alpha_0) \cap \Delta = \text{Supp } (\alpha_0 \beta) \cap \Delta = \emptyset \text{ and } \xi \in \Delta,$$

that

$$\xi \in \text{Supp } (\sigma^{-1} \beta \sigma).$$

Consequently there exist τ_i, τ_j with

$$\sigma^{-1} \tau_i \sigma \tau_j = \xi$$

or

$$\sigma^{-1} \tau_i \sigma = \xi \tau_j^{-1}.$$

But this means that $\sigma \in H_i \sigma_{ij}$.

Therefore we have shown that

$$J = \bigcup_{i,j} H_i \sigma_{ij}.$$

Hence by the preceding lemma, for some index i , $[J: H_i] < \infty$. But $H_i \subseteq C(\tau_i)$, so $[G: C(\tau_i)] < \infty$. This is the required contradiction since $\tau_i \notin \Delta$.

LEMMA 9. Let $S = \{x_1, x_2, \dots, x_n\}$ be a finite normal subset of G . If $H = \langle S \rangle$ the subgroup generated by S then H is normal in G and for all $\sigma \in H$,

$$\sigma = x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}$$

for some integers m_1, m_2, \dots, m_n . In particular, if each x_i is of finite order, then so is H .

Proof. Clearly, H is normal.

Any element of H can be written in the form

$$w = x_{i_1}^{+1} x_{i_2}^{+1} \cdots x_{i_t}^{+1},$$

and we prove the result by induction on the length t of the word. For $t = 1$ there is nothing to prove.

Consider the smallest subscript occurring in the representation of w . Name it j . Then

$$w = w_1 x_j^{+1} w_2 = x_j^{+1} (x_j^{-1} w_1 x_j^{+1}) w_2 = x_j^{+1} w_3,$$

since S is normal.

But w_3 has one less element, so we can write

$$w_3 = x_k^{m_k} x_{k+1}^{m_{k+1}} \cdots x_n^{m_n},$$

omitting the first terms with zero exponent.

If $j \leq k$, we are through. Otherwise, there exists an element of smaller subscript in this representation of w , and we apply this process again. Clearly this procedure terminates after a finite number of applications since S is finite, and the desired result follows.

Proof of Theorem III. Suppose H is a finite normal subgroup of G with order divisible by p for some $p \in \pi(R)$. Choose a nonzero $r \in R_p$, and set

$$\alpha = \sum_{h \in H} rh \in R[G].$$

Then α is nilpotent and central in $R[G]$, so it generates a nilpotent ideal.

Conversely, let N be a nontrivial nilpotent ideal of $R[G]$. Suppose

$$N^m \neq (0), \quad N^{m+1} = (0).$$

For some $p \in \pi(R)$, the projection of N^m into $R_p[G]$ is nonzero. We choose α in this image with $\theta(\alpha) \neq 0$.

Then for all $\sigma \in G$,

$$\sigma^{-1}\alpha\sigma = 0,$$

so by Lemma 8, $\alpha_0 = \psi(\alpha)$ is nilpotent. But $\theta(\alpha_0) = \theta(\alpha) \neq 0$. Thus by Lemma 3, $\text{Supp } \alpha_0$ contains a p element λ . Now $\lambda \in \Delta$, and if we let S be the finite set of conjugates of λ , then S is normal. By the preceding lemma, $H = \langle S \rangle$ is a finite normal subgroup of G with order divisible by p , since $\lambda \in H$. This completes the proof.

We now consider the question of the semi-simplicity of the group algebra $K[G]$. We let $\text{Rad } \Gamma$ denote the Jacobson radical of any ring Γ .

THEOREM IV. *Let K be a field of characteristic $p > 0$, and let G have no elements of order p . If K is a separably generated non-algebraic extension of some subfield K_0 , then $K[G]$ is semi-simple.*

THEOREM V. (Amitsur [1]) *Let K be a field of characteristic zero. If K is a non-algebraic extension of the rational numbers, then for all groups G , $K[G]$ is semi-simple.*

Proof. We consider the first result. Let $(x) = (x_\mu)$ be a transcendence base for K over K_0 . This base is not assumed to be finite but just non-empty. Set $K_1 = K_0(x)$. Then by Theorem II of [2],

$$\text{Rad } K_1[G] \subseteq K_1 \otimes_{K_0} \text{Nil } K_0[G],$$

and since the nil radical is zero by Theorem I above, $K_1[G]$ is semi-simple.

But now K is a separable algebraic extension of K_1 , and by Theorem I of [2],

$$\text{Rad } K[G] = K \otimes_{K_1} \text{Rad } K_1[G].$$

So $\text{Rad } K[G] = 0$, and $K[G]$ is semi-simple.

Theorem V follows similarly.

The latter theorem asserts, in particular, the semi-simplicity of all group algebras over nondenumerable fields of characteristic zero. However the former one does not yield a corresponding result for characteristic $p > 0$ because of the separability condition. But this result can be obtained as follows.

LEMMA 10. *Let H be a subgroup of G , and let $a \in K[H]$. If a is quasi-regular in $K[H]$, then it is in $K[H]$.*

Proof. This follows immediately because the projection of any quasi-inverse of a into $K[H]$ is also a quasi-inverse of a .

THEOREM VI. *Let K be a nondenumerable field of characteristic $p > 0$, and let G be a group having no elements of order p . Then $K[G]$ is semi-simple.*

Proof. Let

$$a = \sum k_G \sigma \in \text{Rad } K[G],$$

and let H be the subgroup of G generated by $\text{Supp } a$. Then H is finitely generated, and $a \in K[H]$. If b is any element of $K[H]$, then ba is quasi-regular in $K[G]$, and hence in $K[H]$, by the preceding lemma. Thus $a \in \text{Rad } K[H]$. But $K[H]$ is a finitely generated algebra over a nondenumerable field. Thus, by Corollary 4 of [3], $a \in \text{Nil } K[H]$. By Theorem I, the nil radical is zero, and thus $a = 0$.

Therefore with the assumption that G has no elements of order p , the basic results of [1] carry over to fields of characteristic $p > 0$.

REFERENCES

1. S. A. Amitsur, *On the semi-simplicity of group algebras*, Michigan Math. J. 6 (1959), 251-253.
2. ———, *The radical of field extensions*, Bull. Res. Council Israel. Sect. F 7F (1957/8), 1-10.
3. ———, *Algebras over infinite fields*, Proc. Amer. Math. Soc. 7 (1956), 35-48.

Harvard University